

Optimal Encoding Capacity of a Linear Optical Quantum Channel

J. A. Smith,¹ D. B. Uskov,^{1,2} and L. Kaplan¹

¹*Tulane University, Department of Physics, New Orleans, Louisiana 70118, USA*

²*Brescia University, Department of Mathematics and Natural Science, Owensboro, Kentucky 42301, USA*

(Dated: August 12, 2015)

Here, we study the classical information capacity of a quantum channel, assuming linear optical encoding, as a function of available photons and optical modes. We present a formula for general channel capacity and show that this capacity is achieved without requiring the use of entangling operations typically required for scalable universal quantum computation, e.g. KLM measurement-assisted transformations. As an example, we provide an explicit encoding scheme using the resources required of standard dense coding using two dual-rail qubits (2 photons in 4 modes). In this case, our protocol encodes one additional bit of information. Greater gains are expected for larger systems.

PACS numbers: 03.67.Hk, 03.67.Ac, 89.70.Kn, 42.79.Sz

I. INTRODUCTION

Superdense coding is an elegant application of basic quantum mechanics that can provide exciting gains in the capacity of an information channel. A simple protocol proposed in 1992 by Bennett and Wiesner proved that two classical bits of information could be sent over a quantum channel via a single qubit [1], a compression made possible by exploiting entanglement as a physical resource. Entanglement can manifest in many forms and in a variety of physical hosts; engineering an entangled system to be used as an efficient communication channel thus presents an interesting challenge. In general, an optimal quantum channel will require a well-devised protocol to properly manipulate a maximally entangled state [2].

We focus here on a linear optical [3] quantum communication channel constructed from a set of modes and photon quanta. The Hilbert space dimension for such a system of N total photons propagating in M optical modes is given by

$$d_H = \frac{(N + M - 1)!}{N!(M - 1)!}, \quad (1)$$

or the number of ways to place N photons in M modes. Considering, for example, a system of two dual-rail qubits ($N = 2$, $M = 4$), we note that $d_H = 10$ whereas the logical qubit space is only four-dimensional. Resource efficiency is paramount in communication and such overhead immediately limits channel capacity. In this paper, we aim to develop optimal dense coding protocols specifically for a linear optical quantum channel, without imposing the qubit as an operational basis.

The protocol requires that Alice and Bob initially share an entangled state of N photons, $|\psi_1\rangle$, with M_A out of the total M modes under Alice's control. Alice chooses a classical symbol x and encodes it by operating on her modes, taking $|\psi_1\rangle$ to $|\psi_x\rangle$. Her resources are forwarded to Bob, who then performs a quantum measurement on the entire state and reads out a classical bit string. Refer to Fig. (1). d_H serves as an absolute upper bound

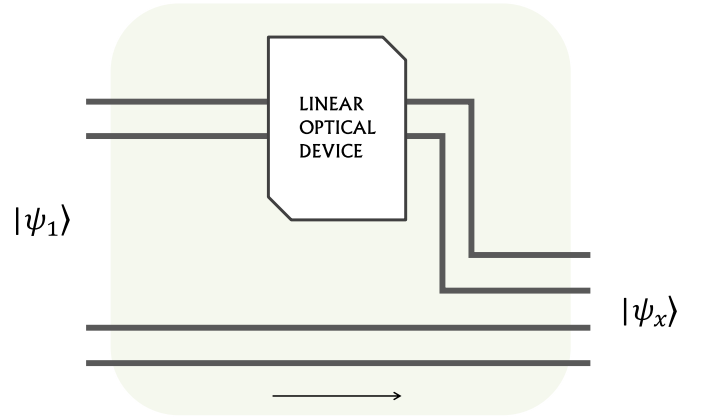


FIG. 1: (Color online) A typical quantum optical encoding device consisting of 4 modes. 2 modes have been distributed to Alice (top), and 2 modes have been distributed to Bob (bottom). Alice applies a linear optical operation and sends her resources to Bob who performs a measurement on the total state.

on the number of distinguishable states Alice can send, though due to the restriction of utilizing only linear optical operations (beam splitters and phase shifters), Alice may not be able to make use of the entire Hilbert space, even if she possesses all of the modes ($M_A = M$). The crux of the problem is that not all quantum logic operations are guaranteed to be accessible via linear optical transformations. Entangling operations in particular require photons to interact, a task they are notoriously ill-suited for. Solutions to this problem exist, e.g. the use of KLM [4] auxiliary resources or non-linear Kerr media. For now, we omit such components from our system. As we shall determine, linear optics is sufficient to construct a maximally efficient communication channel.

We represent the state of our system in the Fock basis

$$|n_1 n_2 \dots n_M\rangle = \frac{(\hat{a}_1^\dagger)^{n_1} (\hat{a}_2^\dagger)^{n_2} \dots (\hat{a}_M^\dagger)^{n_M}}{\sqrt{n_1! n_2! \dots n_M!}} |0\rangle. \quad (2)$$

A general linear operation can then be expressed as

$$\hat{a}_i^\dagger \rightarrow \sum_{j=1}^{M_A} u_{ij} \hat{a}_j^\dagger \quad \forall i = 1 \dots M_A, \quad (3)$$

where u_{ij} are the matrix elements of a unitary operation U acting on M_A modes. Alice encodes one of $|X|$ classical symbols into the system by generating the appropriate quantum state, $|\psi_1\rangle, |\psi_2\rangle, \dots, |\psi_{|X|}\rangle$. Each state $|\psi_x\rangle$ is constructed by applying a different transformation U_x to the initial entangled state, $|\psi_1\rangle$ (here without loss of generality we will take $U_1 = I$).

The mutual entropy $H(X : Y)$ shared between Alice and Bob is constrained by the Holevo bound, which for pure states can be written as [5, 6]

$$H(X : Y) \leq_1 S(\rho) \leq_2 H(X) \leq_3 \log_2 |X|, \quad (4)$$

where X and Y are the encoding and decoding variables,

$$\rho = \sum_{x=1}^{|X|} p_x |\psi_x\rangle \langle \psi_x|, \quad (5)$$

p_x is the probability of choosing symbol x , $S(\rho)$ is the von Neumann entropy of ρ , and $H(X)$ is the Shannon entropy of Alice's encoding variable. Inequality 1 reflects the fact that depending on Bob's measurement capabilities, he may not be able to access all the information encoded by Alice; it becomes an equality only if Bob can perform arbitrary measurements on words of arbitrary length [6–8]. We return to this point in Sec. VI, and in the following we focus on $S(\rho)$, or the encoding capacity of the channel. Inequality 2 becomes an equality when all contributions $|\psi_x\rangle$ to ρ are orthogonal, and finally inequality 3 becomes an equality when all symbols in X are chosen with equal probability.

II. AN UPPER BOUND ON ENCODING CAPACITY

From Eq. (4), it immediately follows that encoding capacity is limited by the Hilbert space dimension,

$$S(\rho) \leq \log_2(d_H). \quad (6)$$

This inequality provides a valuable reference point, but for our purposes we can derive an even stricter bound on $S(\rho)$. First, we abstractly define d_S as the dimension of the span of the states Alice can generate via linear optical transformations as presented in Eq. (3). The Holevo bound again restricts the encoding capacity,

$$S(\rho) \leq \log_2(d_S) \quad d_S \leq d_H. \quad (7)$$

Then, we note the Hilbert space of our channel can be decomposed into a direct sum

$$\mathcal{H} = \bigoplus_{N_A=0}^N (\mathcal{H}^{A,N_A} \otimes \mathcal{H}^{B,N_B}), \quad (8)$$

where each term represents the subspace corresponding to a fixed distribution of photons between Alice and Bob. N_A is the number of photons in Alice's modes, and $N_B = N - N_A$. Any initial state $|\psi_1\rangle$ can be decomposed into a sum of components

$$|\psi_{N_A}\rangle \in \mathcal{H}^{A,N_A} \otimes \mathcal{H}^{B,N_B}. \quad (9)$$

For each such component we can construct a Schmidt decomposition over a set of $\min(d_H^{A,N_A}, d_H^{B,N_B})$ basis vectors, where d_H^{A,N_A} and d_H^{B,N_B} are the dimensions of \mathcal{H}^{A,N_A} and \mathcal{H}^{B,N_B} respectively. Any operation on Alice's modes will act only on the basis vectors of her subspace. It follows that for any $|\psi_{N_A}\rangle$ where $d_H^{A,N_A} < d_H^{B,N_B}$, Alice has no control over the dimensions of Bob's subspace which are not spanned by the basis vectors of the Schmidt decomposition. Thus, the upper bound for the dimension of the span of the set of states Alice is able to generate within each term of Eq. (8) is given by

$$d_S^{N_A} \leq d_H^{A,N_A} \min(d_H^{A,N_A}, d_H^{B,N_B}). \quad (10)$$

We combine Eqs. (8) and (10) to find the upper bound on the total span d_S for given photon number N and modes $M_A, M_B \geq 1$:

$$d_S \leq \sum_{N_A=0}^N f(N_A), \quad (11)$$

where

$$f(N_A) = g(N_A, M_A) \min(g(N_A, M_A), g(N_B, M_B)), \quad (12)$$

$$g(n, m) = \frac{(n + m - 1)!}{n!(m - 1)!} \quad (13)$$

is the number of ways to distribute n photons over m modes, and $M_B = M - M_A$.

This is a key result; if we combine Eqs. (7) and (11) we find an upper bound on the information capacity for a given physical device. As we will see in Sec. III, we find that the bound obtained here is tight.

III. NUMERICAL TESTING OF ALICE'S ENCODING CAPABILITIES

Eqs. (7) and (11) provide a fully analytic upper bound for the information capacity of an optical channel, but the question remains whether and how this bound can actually be reached using linear optical encoding. To obtain the actual encoding capacity, we numerically maximize $S(\rho)$ over the initial state $|\psi_1\rangle$ and Alice's transformations U_x . We call the result of this optimization S_{max} . Similarly, d_S is computed by evaluating the rank of the density matrix for an ensemble of states generated with a sufficiently large set of random U_x .

For small N and M , the numerical results are fairly straightforward and elegant. Of particular interest is the

case where $N = 2$, $M = 4$, $M_A = 2$, which uses the same physical resources as the standard, two dual-rail qubit dense coding protocol. Here we find that $d_S = 8$, in agreement with the right hand side of Eq. (11). Furthermore, we find that $S_{max} \rightarrow \log_2(d_S) = \log_2(8)$ bits can be achieved by generating $|X| = 8$ completely distinguishable states, see Fig. 2 (Left). In contrast with the standard dense coding protocol, which allows Alice to communicate 2 classical bits via a single photon in two modes, we instead find that Alice is able to send 3 classical bits via 1.25 photons (2.4 bits per photon or 1.5 bits per optical mode). This is an important result; Alice is able to encode additional information into the channel by not restricting herself to the qubit basis. The advantage gained by expanding the optimization space beyond the dual rail basis has been consistently observed in other work on gate optimization [9] and photonic quantum communication [10].

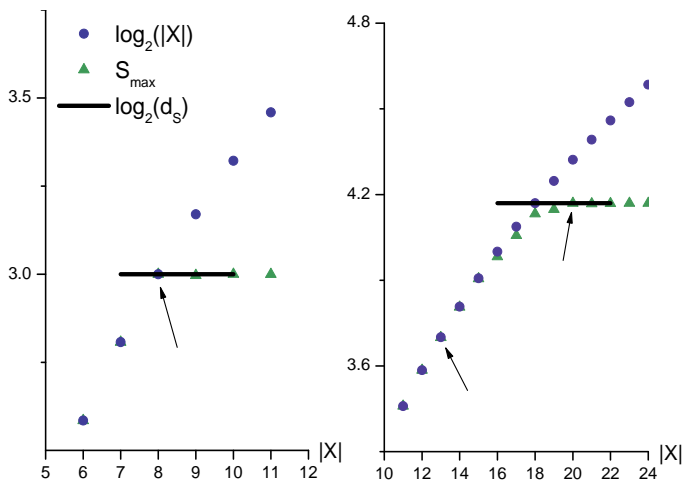


FIG. 2: (Color online) Maximization of the von Neumann entropy $S(\rho)$ as a function of the number of symbols $|X|$. (Left) $N = 2$, $M = 4$, $M_A = 2$. A clear convergence to $\log_2(8) = 3$ is observed. (Right) $N = 3$, $M = 5$, $M_A = 2$. Here S_{max} reaches $\log_2 |X|$ for $|X| \leq 13$, indicating that up to 13 orthogonal states may be generated. Globally, S_{max} reaches $\log_2(18)$ at $|X| = 20$. Analytic solutions can be constructed for $|X| \leq 13$.

For larger, more resource-intensive systems, such straightforward convergence of S_{max} to $\log_2 |X|$ is not observed. We instead find an intermediate optimization regime where the encoding capacity is achieved by increasing the number of coded states $|X|$ beyond the number of orthogonal states Alice can send. As an example, we present the results for $N = 3$, $M = 5$, $M_A = 2$ in Fig. 2 (Right). Here, we find $d_s = 18$ [again in agreement with the right hand side of Eq. (11)] and indeed $S_{max} \rightarrow \log_2(d_S) = \log_2(18)$, but only when $|X| \geq 20$. The maximum channel capacity is equivalent to one associated with 18 orthogonal quantum states, however Alice cannot generate 18 such states using linear optics.

Instead, she must generate a set of at least 20 non-orthogonal states to obtain the maximum capacity of the channel. It becomes apparent that Alice cannot, in general, construct a set of d_S orthonormal basis vectors over the entire subspace accessible to her via allowed optical transformations. She must instead saturate the system with additional linearly independent states until she reaches the potential of the hardware.

In Fig. 3, we present a larger system, $N = 3$, $M = 6$, $M_A = 3$, where $d_S = 38$. Here the full encoding capacity $\log_2 d_S$ is approached slowly as the number of symbols increases, although a modest number of symbols is sufficient to attain a very large fraction of the maximum capacity.

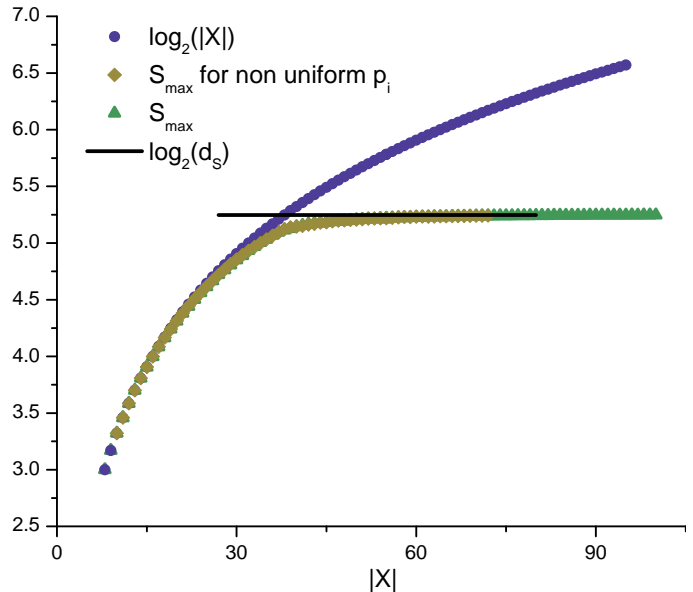


FIG. 3: (Color online) Maximization of the von Neumann entropy for $N = 3$, $M = 6$, $M_A = 3$. $|X|$ must be increased well beyond $d_S = 38$ for the von Neumann entropy S_{max} to maximize to $\log_2(38)$. No gain in information capacity is observed if we allow Alice to send symbols from X with non-uniform probability.

Empirically, we observe in all cases that d_S and S_{max} do attain the upper bounds defined in Eq. (11) and Eq. (7), respectively, assuming only linear optical encoding. We therefore define classical information capacity C in bits per channel use as a function of N, M, M_A :

$$C(N, M, M_A) = \log_2(d_S) = \log_2 \left(\sum_{N_A=0}^N f(N_A) \right), \quad (14)$$

where $f(N_A)$ is defined in Eq. (12). Because the bound in Eq. (11) holds for *any* photon-number preserving operation on Alice's modes, the use of non-deterministic or non-linear entangling optical components will not improve channel capacity.

IV. ASYMPTOTIC BEHAVIOR OF THE ENCODING CAPACITY

To gain some insight into the parameter dependence implied by Eq. (14), we consider the thermodynamic limit $M = \alpha N$, for $M_A, N_A, M_B, N_B, M, N \gg 1$. Applying Stirling's approximation, the full Hilbert space dimension is given by

$$\log_2 d_H \simeq N[\log_2(1 + \alpha) + \alpha \log_2(1 + \alpha^{-1})]. \quad (15)$$

Similarly,

$$\log_2 g(n, m) \simeq m \log_2(1 + \frac{n}{m}) + n \log_2(1 + \frac{m}{n}), \quad (16)$$

and thus N_A^p , the maximum of $g(N_A, M_A)g(N_B, M_B)$, is given by

$$N_A^p \simeq NM_A/M. \quad (17)$$

Now $f(N_A)$ is piecewise defined with the crossover point N_A^c determined by M_A . One can verify that $N_A^p > N_A^c$ if $\frac{M_A}{M_B} > 1$, $N_A^p = N_A^c$ if $\frac{M_A}{M_B} = 1$, and $N_A^p < N_A^c$ if $\frac{M_A}{M_B} < 1$. Thus, the value of $f(N_A)_{max}$ is dependent on the ratio of modes M_A/M_B . We find the following regimes of behavior as a function of the mode ratio M_A/M_B :

$$\frac{M_A}{M_B} > 1 \Rightarrow N_A^p > N_A^c \Rightarrow d_S \simeq d_H \quad (18)$$

$$\frac{M_A}{M_B} = 1 \Rightarrow N_A^p = N_A^c = \frac{N}{2} \Rightarrow d_S \simeq \frac{d_H}{2} \quad (19)$$

$$\frac{M_A}{M_B} < 1 \Rightarrow N_A^p < N_A^c \Rightarrow d_S \ll d_H \quad (20)$$

$$M_B \geq g(N-1, M_A) \Rightarrow d_S \simeq g^2(N-1, M_A) \ll d_H \quad (21)$$

In particular, we see from Eq. (18) that Alice maintains near absolute control of the channel in the range $M_A/M_B > 1$, and the maximum encoding capacity is asymptotically indistinguishable from the capacity implied by the total Hilbert space dimension d_H . Eq. (19) indicates that when the modes are evenly split between Alice and Bob, the maximum encoding capacity is asymptotically lower by precisely one bit than the capacity implied by d_S . From Eq. (21), we find that for a fixed number of modes M_A controlled by Alice, any modes Bob possesses in excess of $g(N-1, M_A)$ do not contribute to channel capacity.

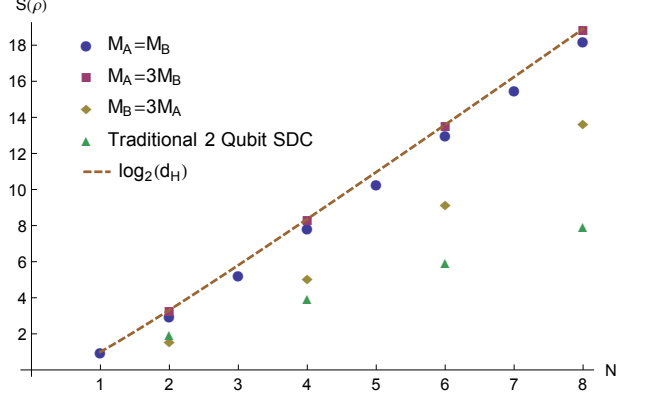


FIG. 4: (Color online) Encoding capacity $\log_2 d_S$ for $M = 2N$ and different ratios M_A/M_B . As an upper and lower bound, we include, respectively, the Hilbert space dimension and the capacity of traditional dense coding using two dual-rail qubits (which assumes $M_A = M_B$).

V. DEVELOPING EXPLICIT ENCODING PROTOCOLS

Thus far we have presented a general method for calculating the information capacity of linear optical hardware. An important task remains; we must be able to design a dense coding protocol for actual implementation. We return to the prototypical case: $N = 2$, $M = 4$, $M_A = 2$. Using the results of the numerical optimization of $S(\rho)$, we find the general set of initial states and transformations that satisfy $\langle \psi_i | \psi_j \rangle = 0 \forall i \neq j$. The result is a non-trivial set of equations, which simplify elegantly if we slightly restrict the space of Alice's transformations, U_3, U_4, \dots, U_8 , see Eq. (22).

VI. DISCUSSION

We have already noted that the Holevo bound is not automatically reachable, and the information capacity of an optical quantum channel is limited by factors other than efficient encoding. The susceptibility of entangled states to decoherence and noise must be considered. Optical quantum computers are an attractive idea in this regard because photons do not strongly interact with most matter; photonic states can thus be carried over large distances [4, 9].

So far we have not addressed the practicality of generating the pre-distributed maximally entangled initial states. The question remains as to whether $|\psi_1\rangle$ can be constructed using deterministic optical components. This will likely depend on the physical resources (N, M, M_A) of a particular device. While deterministic state generation is certainly preferred, it is not essential for efficient communication if one considers cost as that associated with channel usage.

At the receiving end of a quantum channel, signal decoding is an especially challenging task. For the case in which Alice sends orthogonal states, the Holevo bound is achieved by applying an appropriate von Neumann measurement. In principle, a sufficiently large subset of von Neumann measurements can be carried out by having Bob rotate incoming states into the photo-counting basis states (see Lougovski and Uskov [10]). We find that it is not possible to implement such a measurement using deterministic linear optics exclusively. If one were to *impose* a linear optical measurement, Bob would be unable to fully distinguish incoming states [11]. To make things even more complicated, our results suggest that in order to optimize $S(\rho)$, Alice will often send a set of non-orthogonal states. Thus, even if we were able to ap-

ply an optimal POVM, $H(X : Y)$ would fall well below $S(\rho)$ for a single communication [5, 12]. Achieving the Holevo bound for an *a priori* set of non-distinguishable quantum states is a common challenge for quantum information theory, and has been the subject of some study. Proposed solutions [6–8, 13] rely on sending code words comprised of multiple states, $|\psi_a\psi_b\dots\rangle$. For example, the PGM [6] scheme guarantees that a word composed of l states carries $H(X : Y) = lS(\rho)$ information for a coding vocabulary in the limit of large l . The caveat is that Bob must store previously sent letters in a quantum memory storage device, so that he may act on an entire word with a joint measurement. This could be implemented using lM storage modes and a rail-switching junction for incoming letters.

Initial entangled state:

$$|\psi_1\rangle = c_1 e^{id_1} |2000\rangle + c_2 e^{id_2} |1100\rangle + c_3 e^{id_3} |1010\rangle + c_4 e^{id_4} |1001\rangle + c_5 e^{id_5} |0200\rangle \\ + c_6 e^{id_6} |0110\rangle + c_7 e^{id_7} |0101\rangle + c_8 e^{id_8} |0020\rangle + c_9 e^{id_9} |0011\rangle + c_{10} e^{id_{10}} |0002\rangle .$$

Alice's operations:

$$U_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad U_2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \\ U_x = \begin{pmatrix} i(-1)^x \sqrt{\frac{1}{3}} & -\sqrt{\frac{2}{3}} e^{-iq_x} \\ \sqrt{\frac{2}{3}} e^{iq_x} & i(-1)^{x+1} \sqrt{\frac{1}{3}} \end{pmatrix} \quad (x = 3, 4, \dots, 8) \\ q_x = q_3 + \frac{\pi}{3}(x-3) \quad (x = 4, \dots, 8) \quad (22)$$

Restricted by:

$$c_1^2 + c_2^2 + c_5^2 = \frac{3}{8} \quad c_3 = c_7 \quad c_4 = c_6 \quad c_3^2 + c_4^2 = \frac{1}{4} \quad c_8^2 + c_9^2 + c_{10}^2 = \frac{1}{8} \\ d_3 + d_7 - d_4 - d_6 = m\pi \quad m \in \mathbb{Z}_{odd} \\ c_1 c_2 \cos(d_1 - d_2 - q_3) - c_1 c_5 \sin(d_1 - d_5 - 2q_3) - c_2 c_5 \cos(d_2 - d_5 - q_3) = 0 \\ c_1 c_2 \sin(d_1 - d_2 - q_3) - c_1 c_5 \cos(d_1 - d_5 - 2q_3) - c_2 c_5 \sin(d_2 - d_5 - q_3) = 0$$

VII. CONCLUSION

In summary, we have shown that hardware-specific coding algorithms must be developed in order to make full use of a linear optical quantum channel. In Eq. (14), we obtained a simple expression for channel capacity as a function of photons and optical modes. Furthermore, we found this capacity is achievable via *some* encoding procedure using linear optics exclusively. We observe that for small systems, Alice can send completely distinguishable states. Generally, however, Alice must choose from a pool of non-orthogonal states. In either case, it is possible to extract an encoding protocol from the numerical maximization of the von Neumann entropy.

Acknowledgments

We are grateful for helpful discussions with Nick Sparks and Pavel Lougovski. This work was supported in part by the NSF under Grants PHY-1005709 and PHY-1205788. DBU acknowledges support from AFRL Information Directorate under grant FA 8750-11-2-0218. This research was supported in part using high performance computing (HPC) resources and services provided by Technology Services at Tulane University.

-
- [1] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
 - [2] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).
 - [3] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, Rev. Mod. Phys. **79**, 135 (2007).
 - [4] E. Knill, R. Laflamme, G. J. Milburn, Nature (London) **409**, 46 (2001).
 - [5] A. S. Holevo, Probl. Peredachi Inf. **9**, 110 (1973).
 - [6] P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland, and W. K. Wootters, Phys. Rev. A **54**, 1869 (1996).
 - [7] V. Giovannetti, S. Lloyd, and L. Maccone, Phys. Rev. A **85**, 012302 (2012).
 - [8] S. Lloyd, V. Giovannetti, and L. Maccone, Phys. Rev. Lett. **106**, 250501 (2011).
 - [9] D. B. Uskov, A. M. Smith, and L. Kaplan, Phys. Rev. A **81**, 012303 (2010).
 - [10] P. Lougovski and D. B. Uskov Phys. Rev. A **92**, 022303 (2015).
 - [11] K. Mattle, H. Weinfurter, P.G. Kwiat, and A. Zeilinger, Phys. Rev. Lett. **76**, 4656 (1996).
 - [12] A. Peres and W. K. Wootters, Phys. Rev. Lett. **66**, 1119 (1991).
 - [13] T. Ogawa and H. Nagaoka, IEEE Trans. Inf. Theory **53**, 2261 (2007).